FCWCOM
YOUR GOVERNMENT IT RESOURCE

e-business

Airport security tech scrutinized

BY Dibya Sarkar
June 17, 2002

Printing? Use this version.
Email this to a friend.

A task force charged with reviewing current and emerging technologies to improve security at the San Jose, Calif., airport has prepared a report that could have national implications.

The report, which will be submitted today to the city council and the federal Transportation Security Administration (TSA), focuses on promising technologies that could address passenger convenience, security and cost, said John Thompson, chairman and chief executive officer of Symantec Corp. and chairman of the task force, which was convened by San Jose Mayor Ron Gonzales and U.S. Rep. Mike Honda (D-Calif.).

Although the group's first objective was to improve security at Norman Y. Mineta San Jose International Airport, Thompson said local officials want TSA to select the airport as one of 20 pilot sites to receive funding for such security measures. TSA officials have already decided to study security procedures at about 15 airports.

He said other airports across the country also could adopt the task force's recommendations. "I think what's good about this report is that it frames the problem and gives a prescription in application areas as opposed to just running on about technology, retinal scanning, biometrics, and on and on and on and on," he said.

"What we concluded was that technology certainly can be applied to the issue of protecting the airports.... But it is as much about process as it is

RELATED LINKS

The 2002 Silicon Valley Blue Ribbon Task Force on Aviation Security and Technology

Transportation Security Administration

"TSA preps smart card program" [Federal Computer Week, June 10, 2002]

"TSA readies network pact" [Federal Computer Week, May 20, 2002]

"TSA preps $1B-plus IT buy" [Federal Computer Week, May 14, 2002]

"TSA trounced over spending" [Federal Computer Week, April 19, 2002]

technology," Thompson said. "How do you respond when there's an incident? That's not technology. That's as much about having policies and practices that are well articulated, well understood by everyone involved and rigorously adhered to."

The report is divided into three broad areas, with technologies highlighted for each. The areas are:

* Creating a trusted or validated facility by using technologies to secure the perimeter of the airport, its buildings, and access into and out of certain sections.

* Creating a trusted employee program using appropriate clearances and authentication. Such a system also could be applied to a "validated passenger" program, Thompson said.

* Creating a trusted network. "Airports today operate somewhat in isolation and somewhat on open or unsecured networks," he said. "And so there's a need to create a way to link airports and information about what's going on in an airport onto a digitized network."

The group looked at current technologies to help "mitigate or solve the problem today as we know it," he said, "and then we looked at concepts or technologies that are further out that require further exploration for which someone might want to have an ongoing vigilant look."

To do this, the report recommended a research and development focus within TSA, the U.S. Transportation Department or another appropriate agency "so systems don't become stale," he said.

Cost is another critical issue, he added.

"Much of what happens in an airport is controlled and funded by the local authorities from a security point of view," he said. "And so before we as a task force would mandate or suggest [that] these technologies could work, somewhere along the way the process needs to be made clear as to where the money's going to come from to ensure that we do in fact improve the security of the airport."

Addressing the cost factor, Honda said, "Certainly the TSA and other agencies involved with security will probably be participating in covering the costs. But the government cannot carry all the costs itself, and that's why public/private partnerships are going to be critical."

Honda cited the task force itself as an example of public/private cooperation. "I think that this blue-ribbon task force is a good example of applying entrepreneurial spirit to protect a democracy that depends heavily on public and private partnerships," he said.

Task force members included technology and airline executives as well as representatives from higher education, law enforcement and the federal government. The task force held a public hearing that drew about 75 participants and received proposals from more than 40 companies.